

What is claimed is:

- Sub B9
- 1 1. In a system having one or more security mechanisms, a method of defining and
2 enforcing a security policy, the method comprising:
3 encapsulating security mechanism application specific information for each
4 security mechanism, wherein encapsulating includes forming a key for each security
5 mechanism;
6 combining keys to form key chains;
7 encapsulating key chains as keys and passing the key chain keys to another
8 semantic layer;
9 defining the security policy, wherein defining includes forming key chains from
10 keys and associating users with key chains;
11 translating the security policy and exporting the translated security policy to the
12 security mechanisms; and
13 enforcing the security policy via the security mechanisms.
- 1 2. The method of claim 1 wherein the security mechanisms are located on one or
2 more distributed computer networks.
- 1 3. The method of claim 1 wherein the security mechanisms are heterogeneous.
- 1 4. The method of claim 1, wherein defining the security policy further includes
2 drilling down into a next lower semantic layer to form a new key chain.
- 1 5. The method of claim 1 wherein the security policy is defined using a graphical
2 user interface.
- 1 6. A security system comprising:
2 a plurality of security mechanisms;

3 a plurality of semantic layers, including a first semantic layer, wherein the first
4 semantic layer combines keys, wherein each key encapsulates security mechanism
5 application specific information for a security mechanism;
6 a user interface for defining a security policy as a function of keys received from
7 a lower semantic layer; and
8 a translator for translating the security policy to the security mechanisms.

1 7. The system according to claim 6 wherein the user interface is a graphical user
2 interface.

1 8. The system according to claim 6 wherein the security policy is a role-based
2 access control model.

1 9. The system of claim 6 wherein the semantic layers form a poset.

1 10. The system of claim 6 wherein the user interface includes means for drilling
2 down into a lower semantic layer to form a new key chain.

1 11. A security system comprising:
2 a model comprising one or more semantic layers for defining different security
3 policies and constraints for each type of user;
4 a tool for manipulating the model; and
5 a translator for translating security policies from the model to security
6 mechanisms in one or more computer resources.

1 12. The method of claim 11 wherein the model comprises a static application policy
2 layer, one or more semantic policy layers, and a dynamic local policy layer.

1 13. The method of claim 11 wherein the model represents a set of access rights for a
2 computer resource as a key and the model represents a set of keys as a key chain.

1 14. A method of defining a security policy, the method comprising:
2 defining an application policy layer and a plurality of semantic policy layers,
3 including a first semantic policy layer and a second semantic layer;
4 encapsulating a set of access rights for a computer resource as a key;
5 combining keys to form one or more key chains within the application policy
6 layer;
7 exporting key chains in the application policy layer as a key;
8 importing at least one key from the application policy layer into the first
9 semantic policy layer;
10 combining one or more keys in the first semantic policy layer to form a key
11 chain;
12 exporting key chains in the first semantic policy layer as keys;
13 importing at least one key into the second semantic policy layer;
14 combining one or more keys in the second semantic policy layer to form a key
15 chain;
16 exporting key chains in the second semantic policy layer as keys;
17 importing at least one key from the second semantic policy layer to a local
18 policy layer;
19 combining one or more keys in the local policy layer to form one or more local
20 policy key chains; and
21 assigning users to local policy key chains in the local policy layer.

1 15. The method of claim 14 wherein combining one or more keys to form a key
2 chain includes combining a key chain with the one or more keys to form another key
3 chain.

1 16. The method of claim 14 wherein combining one or more keys in the first
2 semantic layer includes combining a key chain with the one or more keys to form
3 another key chain.

1 17. The method of claim 14 wherein combining one or more keys to form a key
2 chain includes associating a constraint with the key chain, wherein the constraint must
3 be satisfied before access to a computer resource governed by the key chain is granted.

1 18. The method of claim 14 wherein encapsulating includes grouping methods into
2 handles and handles into keys.

1 19. The method of claim 18 wherein each key chain includes handles for different
2 computer resources.

1 20. The method of claim 14 wherein combining one or more keys to form a key
2 chain includes marking the key chain as abstract, wherein key chains marked as abstract
3 are not exported to other layers.

1 21. The method of claim 14 further comprising combining one or more keys and
2 key chains in the local policy layer to form a new key chain in the local policy layer.

1 22. A method of defining a security policy, the method comprising:
2 defining an application policy layer and a semantic policy layer;
3 encapsulating a set of access rights for a computer resource as a key;
4 combining keys to form one or more key chains within the application policy
5 layer;
6 exporting key chains in the application policy layer as a key;
7 importing at least one key from the application policy layer into the semantic
8 policy layer;
9 combining one or more keys in the semantic policy layer to form a key chain;
10 exporting key chains in the semantic policy layer as keys;
11 importing at least one key from the semantic policy layer to a local policy layer;

12 combining one or more keys in the local policy layer to form one or more local
13 policy key chains; and
14 assigning users to local policy key chains in the local policy layer.

1 23. The method of claim 22 wherein combining one or more keys in the semantic
2 policy layer to form a key chain includes combining a key chain with the one or more
3 keys to form another key chain.

1 24. The method of claim 22 wherein combining one or more keys in the local policy
2 layer to form a key chain includes combining a key chain with the one or more keys to
3 form another key chain.

1 25. The method of claim 22 wherein combining one or more keys in the semantic
2 policy layer to form a key chain includes associating a constraint with the key chain,
3 wherein the constraint must be satisfied before access to a computer resource governed
4 by the key chain is granted.

1 26. The method of claim 22 wherein combining one or more keys in the local policy
2 layer to form a key chain includes associating a constraint with the key chain, wherein
3 the constraint must be satisfied before access to a computer resource governed by the
4 key chain is granted.

1 27. The method of claim 22 wherein encapsulating includes grouping methods into
2 handles and handles into keys.

1 28. The method of claim 27 wherein each key chain includes handles for different
2 computer resources.

1 29. The method of claim 22 wherein combining one or more keys to form a key
2 chain includes marking the key chain as abstract, wherein key chains marked as abstract
3 are not exported to other layers.

1 30. The method of claim 22 further comprising combining one or more keys and
2 key chains in the local policy layer to form a new key chain in the local policy layer.

1 31. A method of modifying a security policy, the method comprising:
2 defining an application policy layer and a semantic policy layer;
3 encapsulating a set of access rights for a computer resource as a key;
4 combining keys to form one or more key chains within the application policy
5 layer;
6 exporting key chains in the application policy layer as a key;
7 importing at least one key from the application policy layer into the semantic
8 policy layer;
9 combining one or more keys in the semantic policy layer to form a key chain;
10 exporting key chains in the semantic policy layer as keys;
11 importing at least one key from the semantic policy layer to a local policy layer;
12 combining one or more keys in the local policy layer to form one or more local
13 policy key chains;
14 assigning users to local policy key chains in the local policy layer;
15 constructing a role hierarchy by sorting the key chains into a partial ordering
16 based on set containment;
17 displaying the partial ordering as a role hierarchy graph; and
18 adding and deleting keys from the role hierarchy graph.

1 32. An article comprising a computer readable medium having instructions thereon,
2 wherein the instructions, when executed in a computer, create a system for executing the
3 method of claim 1.

1 33. An article comprising a computer readable medium having instructions thereon,
2 wherein the instructions, when executed in a computer, create a system for executing the
3 method of claim 14.

1 34. An article comprising a computer readable medium having instructions thereon,
2 wherein the instructions, when executed in a computer, create a system for executing the
3 method of claim 22.

1 35. An article comprising a computer readable medium having instructions thereon,
2 wherein the instructions, when executed in a computer, create a system for executing the
3 method of claim 31.

1 36. In a system having a workflow management system and a central policy
2 management system, a method of controlling workflow, comprising:
3 creating a workflow class definition;
4 exporting the workflow class definition to the central policy management
5 system;
6 binding resources and roles to steps within the central policy management
7 system;
8 creating a workflow instance in both the workflow management system and the
9 central policy management system; and
10 executing the workflow instance.

1 37. An article comprising a computer readable medium having instructions thereon,
2 wherein the instructions, when executed in a computer, create a system for executing the
3 method of claim 36.

1 38. A workflow control system, comprising:
2 a workflow management system; and
3 a central policy management system;

